CLAIMS

What is claimed is:

1. A method for establishing secured roaming among a wireless station, a first and a second access points, comprising:

   a. the first access point requesting a first ticket from an authentication server and using the first ticket to establish a first secured session with the wireless station; and

   b. in response to a second ticket request from the wireless station through the first secured session, the first access point forwarding the second ticket request to the authentication server and relaying a resulting second ticket from the authentication server to the wireless station.

2. The method according to claim 1, the method further comprises: applying the second ticket and a group identity shared by the first and the second access points to establish a second secured session between the wireless station and the second access point.

3. The method according to claim 1, the method further comprises:

   a. the authentication server dynamically generating a first and a second session keys to include in the first and the second tickets, respectively;

and

b. the authentication server encrypting the first and the second tickets with a first and a second encryption keys.

4. The method according to claim 3, the first and the second session keys have limited lifetime.

5. The method according to claim 3, the method further comprises:

a. the first access point appending application specific information to the second ticket to formulate a combined message; and

b. the first access point encrypting the combined message with the first session key.

6. The method according to claim 5, the application specific information further comprises the first access point's selected time and random number.

7. An access point in a secured wireless roaming system, comprising:

a. an antenna;

b. a filter coupled to the antenna;

c. a receiver and a transmitter coupled to the filter; and

d. a control unit coupled to the receiver and the transmitter and coupled to a wired-network connection interface, wherein the control unit further comprises an authentication protocol engine that

i. requests a first ticket from an authentication server and uses the first ticket to establish a first secured session with a wireless station; and

ii. in response to a second ticket request from the wireless station through the first secured session, forwards the second ticket request to the authentication server and relays a resulting second ticket from the authentication server to the wireless station.

8. The access point according to claim 7, the control unit further comprises: an encryption/decryption engine to decrypt the second ticket request before the authentication protocol engine forwards the second ticket request.

9. The access point according to claim 7, wherein the authentication server further:

a. dynamically generates a first and a second session keys to include in the first and the second tickets, respectively; and

b. encrypts the first and the second tickets with a first and a second encryption keys.

10. The access point according to claim 9, the first and the second session keys have limited lifetime.

11. The access point according to claim 8, further comprises:

a. the authentication protocol engine to append application specific information to the second ticket to formulate a combined message; and

b. the encryption/decryption engine to encrypt the combined message with the first session key.

12. The access point according to claim 11, the application specific information further comprises the access point's selected time and random number.

13. A wireless station in a secured wireless roaming system, comprising:

a. an antenna;

b. a filter coupled to the antenna;

c. a receiver and a transmitter coupled to the filter; and

d. a control unit coupled to the receiver and the transmitter, wherein the

control unit further comprises an authentication protocol engine that requests a second ticket from an authentication server via an access point after having used a first ticket to establish a first secured session with the access point.

14. The wireless station according to claim 13, comprising:

the authentication protocol engine to apply the second ticket and a group identity shared by the first and a second access points to establish a second secured session with the second access point.

15. A secured wireless roaming system, comprising:

a wired medium;

a wireless medium;

an authentication server coupled to the wired medium;

a wireless station coupled to the wireless medium; and

an access point coupled to the wireless medium and the wired medium, wherein the access point comprises:

i. a first control unit, comprising a first authentication protocol engine to request a first ticket from the authentication server and use the first ticket to establish a first secured session with the

wireless station; and

ii. in response to a second ticket request from the wireless station through the first secured session, to forward the second ticket request to the authentication server and relays a resulting second ticket from the authentication server to the wireless station.

16. The secured wireless roaming system according to claim 15, wherein the wireless station further comprises:

a second authentication protocol engine to apply the second ticket and a group identity shared by the first and a second access points to establish a second secured session with the second access point.

17. The secured wireless roaming system according to claim 15, the first control unit further comprises:

an encryption/decryption engine to decrypt the second ticket request before the authentication protocol engine forwards the second ticket request.

18. The secured wireless roaming system according to claim 15, wherein the authentication server further:

a. dynamically generates a first and a second session keys to include in the

first and the second tickets, respectively; and

b. encrypts the first and the second tickets with a first and a second encryption keys.

19. The secured wireless roaming system according to claim 17, the first and the second session keys have limited lifetime.

20. The secured wireless roaming system according to claim 17, further comprising:

a. the first authentication protocol engine to append application specific information to the second ticket to formulate a combined message; and

c. the first encryption/decryption engine to encrypt the combined message with the first session key.

21. The access point according to claim 20, the application specific information further comprises the access point's selected time and random number.